Diagonal forms of incidence matrices associated with t-uniform hypergraphs

Richard M. Wilson[1] and Tony W. H. Wong
California Institute of Technology

Abstract

We consider integer matrices $N_t(\mathbf{h})$ whose rows are indexed by the t-subsets of an n-set and whose columns are all images of a particular column $\mathbf{h}$ under the symmetric group S_n. Earlier work has determined a diagonal form for $N_t(\mathbf{h})$ when $\mathbf{h}$ has at least t 'isolated vertices' and the results were applied to the binary case of a zero-sum Ramsey-type problem of Alon and Caro involving t-uniform hypergraphs. This paper deals with the case that $\mathbf{h}$ does not have as many as t isolated vertices.

1 Introduction

By a *t-vector* based on a set X, we mean a vector $\mathbf{h}$ whose coordinates are indexed by the t-subsets of the set X. We use a functional notation: if $\mathbf{h}$ is a t-vector and T a t-subset of X, then $\mathbf{h}(T)$ will denote the entry of $\mathbf{h}$ in coordinate position T.

Given an integer t-vector $\mathbf{h}$ based on an n-set X, we consider the matrix $N_t^n(\mathbf{h})$ or $N_t(\mathbf{h})$, or simply N_t, whose columns are the images of $\mathbf{h}$ under the symmetric group S_n. Normally, one only needs to use the distinct images of $\mathbf{h}$ as the columns of N_t, but, for most purposes, it will not matter if N_t has repeated columns.

Examples of such matrices include integer matrices in the association algebras of Johnson schemes $J(n,t)$. Other examples include the inclusion matrices W_{tk} mentioned in Section 3.

A *diagonal form* for an integer matrix A is an integer diagonal matrix D of the same shape as A, not necessarily square, such that $EAF = D$ for some (square) unimodular matrices E and F. An *isolated vertex* for a t-vector $\mathbf{h}$ is a point x such that $\mathbf{h}(T) = 0$ for every t-subset T containing x. In [11], a diagonal form for $N_t(\mathbf{h})$ is described when $\mathbf{h}$ has at least t isolated vertices. This paper deals with the case that $\mathbf{h}$ does not have as many as t isolated vertices.

Given a simple t-uniform hypergraph H with vertex set X, its *characteristic t-vector* is the t-vector $\mathbf{h}$ based on X defined by $\mathbf{h}(T) = 1$ if T is

[1]The research of the first author was supported in part by NSF Grant DMS-0555755

an edge of H and $\mathbf{h}(T) = 0$ otherwise. In this case, we can write $N_t(H)$ rather than $N_t(\mathbf{h})$. A nonnegative integer t-vector may be regarded as the characteristic t-vector of a t-uniform multihypergraph.

We are able to extend the theorem in [11] to describe a diagonal form for $N_t(H)$ (and more generally for $N_t(\mathbf{h})$) whenever H (or $\mathbf{h}$) has a certain property (that H and all its 'shadows' are multiples of 'primitive' hypergraphs); see Theorem 9 in Section 4. Hypergraphs (or t-vectors) with at least t isolated vertices have this property. This property is shown in Section 5 to hold for almost all t-uniform hypergraphs on k vertices (k large) while only a small proportion of t-uniform hypergraphs have t isolated vertices.

Diagonal forms for $N_2(G)$ are found for all primitive multigraphs G in Section 6 and all simple graphs G in Section 7. Theorem 17 generalizes a result of Brouwer and Van Eijl [2] on the Smith form of the adjacency matrix of the line graph of a complete graph.

The current work is motivated in part by a certain zero-sum Ramsey-type problem introduced by N. Alon and Y. Caro [1]. Let H be a t-uniform hypergraph and let p be a prime. Their problem, in our notation, asks for the smallest number $R_p(H)$ so that, for $n \geq R_p(H)$ the row space of $N_t(H^{\uparrow n})$ over the field of p elements does not contain a nowhere-zero vector. Here $H^{\uparrow n}$ denotes the hypergraph obtained from H by adjoining isolated vertices to H so that the total number of vertices is n. (Such an integer exists by the classical Ramsey's Theorem as long as p divides the number of edges of H.) Thus $R_2(H)$ is the smallest number so that, for $n \geq R_2(H)$, the binary code generated by $N_t(H^{\uparrow n})$ does not contain the vector $\mathbb{1}$ of all 1's.

In general, we consider the problem of deciding when the vector $\mathbb{1}$ is in the row space of $N_t(H)$ over the field of order p. (This applies directly to the zero-sum Ramsey-type problem only when $p = 2$.) Our approach is based on Lemma 2 which explains how a diagonal form D for $N_t(H)$ and the matrices E and F with $EN_tF = D$ can be used to decide whether there exists an integer row vector $\mathbf{y}$ satisfying the system of congruences $\mathbf{y}N_t \equiv \mathbb{1} \pmod{p}$.

The result $R_2(G) \leq k+2$ for graphs with k vertices and an even number of edges, from [1], was greatly refined by Caro [3], who gave the exact value of $R_2(G)$ for any simple graph G. His theorem implies that $R_2(G) = k$ almost always. We use diagonal forms for $N_2(G)$ to reprove this theorem and to extend his result to our problem asking when $\mathbb{1} \in \mathrm{row}_p(N_2(G))$.

Earlier results on diagonal forms of $N_t(H)$ were applied in [12] to prove that for any t-uniform hypergraph with an even number of edges, $R_2(H) \leq k+t$, where k is the number of vertices of H. Here we prove that $R_2(H) = k$ for almost all hypergraphs with an even number of edges, and give our extension for primes $p > 2$; see Section 8.

2 Diagonal form and solutions of systems of congruences

Two integer matrices A and B of the same size are $\mathbb{Z}$-equivalent when there exist unimodular matrices (square integer matrices that have integer inverses, or what is the same have determinants ± 1) E and F so that $EAF = B$. This is equivalent to stating that B can be obtained from A by a sequence of $\mathbb{Z}$-row operations and $\mathbb{Z}$-column operations (permuting rows/columns, adding an integer multiple of one row or column to another row or column, or multiplying a row or column by -1).

Given A, there is a unique diagonal integer matrix D that is $\mathbb{Z}$-equivalent to A such that the diagonal entries $d_1, d_2, d_3, \ldots$ are nonnegative integers and where d_i divides d_{i+1} for $i = 1, 2, \ldots$. Here 'diagonal' means that the (i, j)-entry of D is 0 unless $i = j$, but D has the same shape as A and is not necessarily square. This unique diagonal matrix is called the *integer Smith normal form*, or simply the *Smith form*, of A. (The Smith form D is unique; the unimodular matrices E and F so that $EAF = D$ are not. See [8] for background on Smith form.)

The diagonal entries of the Smith form are called the *invariant factors*, or the *elementary divisors* of A. We call any diagonal matrix D that is $\mathbb{Z}$-equivalent to A a *diagonal form* for A. The diagonal entries of a diagonal form for A will be called (a multiset of) *diagonal factors* for A. The rank of a matrix is the number of nonzero entries in any list of diagonal factors. The number of diagonal factors of an $r \times s$ matrix is the minimum of r and s; but sometimes it will be convenient, in this paper, to speak of diagonal factors $d_1, d_2, \ldots, d_r$ of an $r \times s$ matrix even when $r > s$; in this case it is to be understood that $d_i = 0$ for $s < i \leq r$, as if we replaced the matrix by that obtained by appending $r - s$ columns of all 0's. Diagonal factors of a matrix A are also diagonal factors for $A^\top$, except that the number of 0's may differ, unless we consider only $\min\{r, s\}$ as the number of diagonal factors.

Integers $d_1, d_2, \ldots, d_r$ are diagonal factors for an $r \times s$ matrix A if and only if

$$\mathbb{Z}^r / \mathrm{col}_{\mathbb{Z}}(A) \cong \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}, \tag{1}$$

where $\mathrm{col}_{\mathbb{Z}}(A)$ is the $\mathbb{Z}$-module (abelian group) generated by the columns of A. (Of course, $\mathbb{Z}_1 = \{0\}$ and $\mathbb{Z}_0 = \mathbb{Z}$.) As we mentioned above, it is to be understood that $d_i = 0$ for $s < i \leq r$.

The group in (1) may be called the (column) *Smith group* $S(A)$ of A. The dimension of $S(A)$ as a finitely generated abelian group is the number

of diagonal factors $d_1, \ldots, d_r$ that are equal to 0 and this is $r - \text{rank}(A)$. We use $\tau(A)$ to denote the order of the torsion subgroup of $S(A)$; this is the product of the nonzero diagonal factors.

If the rows of an $r \times s$ integer matrix M are linearly independent over any field, we say M is *row-unimodular*. This is the same as saying that diagonal factors of M consist of r 1's, or that the Smith group of M is trivial. Every row-unimodular matrix M has *unimodular extensions*, i.e. there are unimodular matrices F whose row set includes the rows of M. We remark that rows added to obtain a unimodular extension of a row-unimodular matrix M also provide a unimodular extension of any matrix M' of the same size with $\text{row}_{\mathbb{Z}}(M') = \text{row}_{\mathbb{Z}}(M)$.

The following two lemmas will be used in Sections 7, 8, and 9.

Lemma 1 *Let A be an $r \times s$ integer matrix, $r \leq s$, and E a unimodular matrix with rows $\mathbf{e}_1, \ldots, \mathbf{e}_r$. Suppose $\mathbf{e}_i A$ has all coordinates divisible by an integer d_i, $i = 1, 2, \ldots r$. That is, suppose $EA = DB$ where D is a square diagonal matrix and B is integral. If $\text{rank}(A) = \text{rank}(D)$ and $\tau(A)$ divides $\tau(D)$, then there exists a unimodular matrix F so that $EAF = [D, O]$.*

Proof. The mapping $\mathbf{y} \mapsto E\mathbf{y}$ is an isomorphism from $\text{col}_{\mathbb{Z}}(A)$ onto a subgroup L_0 of $L = d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z}$. Then $S(A) = \mathbb{Z}^r/\text{col}_{\mathbb{Z}}(A)$ has $\mathbb{Z}^r/L = \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_r}$ as a homomorphic image. But, by hypothesis, $S(A)$ and $\mathbb{Z}^r/L$ have the same dimension and the order $\tau(A)$ of the torsion subgroup of $S(A)$ divides the order $\tau(D)$ of the torsion subgroup of $\mathbb{Z}^r/L$. It follows that $S(A)$ and $\mathbb{Z}^r/L$ are isomorphic and that $L_0 = L$, i.e. the mapping $\mathbf{y} \mapsto E\mathbf{y}$ is onto L.

For notational convenience, say that $d_1, d_2, \ldots, d_\ell$ are nonzero and $d_{\ell+1} = \cdots = d_r = 0$ for some $\ell \leq r$. Let D_1 be the $r \times \ell$ matrix consisting of the first ℓ columns of D, and B_1 the $\ell \times s$ matrix consisting of the top ℓ rows of B. Of course, $D_1 B_1 = DB$.

Let $\mathbf{d}_j = [0, \ldots, 0, d_j, 0, \ldots, 0]^\top$ be the j-th column of D. Because the mapping $\mathbf{y} \mapsto E\mathbf{y}$ is onto L, there exists an integer vector $\mathbf{c}_j$ so that $EA\mathbf{c}_j = \mathbf{d}_j$, $j = 1, \ldots, \ell$. Let C be the $s \times \ell$ matrix with columns $\mathbf{c}_j$, $j = 1, \ldots, \ell$. Then $D_1 = EAC = D_1(B_1 C)$, and since the columns of D_1 are linearly independent, $I = B_1 C$. This means B_1 is row-unimodular. Let B_2 be any unimodular completion of B_1. Then $EA = DB = [D, O]B_2$, so $EAF = [D, O]$ where $F = B_2^{-1}$. □

Lemma 2 *Let A be an $r \times s$ integer matrix. Suppose $EAF = D$ where E and F are unimodular and D is diagonal with diagonal entries $d_1, d_2, \ldots, d_s$,*

with the understanding that $d_i = 0$ if $r < i \leq s$. Let $\mathbf{c}$ be an integer row vector of length s. The system of congruences $\mathbf{y}A \equiv \mathbf{c} \pmod{m}$ has an integer solution $\mathbf{y}$ if and only if the j-th entry of $\mathbf{c}F$ is divisible by the gcd of m and d_j, for $j = 1, 2, \ldots, s$.

Proof. The system $\mathbf{y}A \equiv \mathbf{c} \pmod{m}$ is equivalent to $(\mathbf{y}E^{-1})(EA) \equiv \mathbf{c} \pmod{m}$, and this has integer solutions $\mathbf{y}$ if and only if $\mathbf{z}(EA) \equiv \mathbf{c} \pmod{m}$ has an integer solution $\mathbf{z}$. This in turn will have integer solutions if and only if $\mathbf{z}(EAF) \equiv \mathbf{c}F \pmod{m}$, or $\mathbf{z}D \equiv \mathbf{c}F \pmod{m}$, has integer solutions. Since D is diagonal, it is easy to see that this last set of congruences has solutions if and only if the condition of the statement of the lemma holds. □

3 Inclusion matrices and primitivity

For integers t, k, n with $0 \leq t \leq k \leq n$, let W_{tk} or $W_{tk}(n)$ denote the $\binom{n}{t} \times \binom{n}{k}$ matrix whose rows are indexed by the t-subsets of an n-set X, whose columns are indexed by the k-subsets of X, and where the entry in row A and column B is

$$W_{tk}(A, B) := \begin{cases} 1 & \text{if } A \subseteq B, \\ 0 & \text{otherwise.} \end{cases}$$

Integer vectors in the null space $\mathrm{null}_{\mathbb{Q}}(W_{tk})$ of W_{tk} are called *null t-designs* or *trades*. A survey and comparison of explicit constructions of $\mathbb{Z}$-bases for $\mathrm{null}_{\mathbb{Z}}(W_{tk})$ may be found in [7].

The elements of all bases are of a certain type that were called (t, k)-pods by Graver and Jurkat [6], cross-polytopes by Graham, Li, and Li in [5], and minimal trades in [7]. For our purposes, we need only to know a generating set for $\mathrm{null}_{\mathbb{Z}}(W_{t-1,t})$, and we restrict our attention to this case. We use the term *t-pods* for what are called $(t-1, t)$-pods in [6].

Let P be a set of t disjoint ordered pairs

$$\{(a_1, b_1), (a_2, b_2), \ldots, (a_t, b_t)\} \tag{2}$$

of elements of a set X, with union Y, say. We will call such a set P a *pairing*, and to each such pairing we associate a t-pod $\mathbf{f}_P$ defined as follows. For a t-subset $T = \{c_1, c_2, \ldots, c_t\}$ of X, $\mathbf{f}_P(T)$ is to be the coefficient of the monomial $c_1 c_2 \cdots c_t$ in the expansion of the polynomial

$$(a_1 - b_1)(a_2 - b_2) \cdots (a_t - b_t)$$

as the sum of 2^t monomials. Thus $\mathbf{f}_P(T) = 0$ unless T contains exactly one member of each pair $\{a_i, b_i\}$, in which case we call T *transverse* (to P), and for a transverse t-subset T,

$$\mathbf{f}_P(T) = (-1)^{|T \cap \{b_1, b_2, \ldots, b_t\}|}.$$

See [5] or [6] for a proof of Theorem 3 below.

Theorem 3 *Every t-pod is in $\mathrm{null}_{\mathbb{Z}}(W_{t-1,t}(n))$ and every integer t-vector in the null space of $W_{t-1,t}(n)$ is an integer linear combination of t-pods.*

(There are no t-pods if $n < 2t$, but in that case, $\mathrm{null}_{\mathbb{Z}}(W_{t-1,t})$ is trivial, see e.g. [6], so the theorem remains valid.)

Let $\mathbf{h}$ be a t-vector based on a set of at least $2t$ points. We say that $\mathbf{h}$ is *primitive* when the GCD of $\langle \mathbf{f}, \mathbf{h} \rangle$ over all integer t-vectors $\mathbf{f} \in \mathrm{null}_{\mathbb{Z}}(W_{t-1,t})$ is equal to 1. In general, we say that the GCD γ of all $\langle \mathbf{f}, \mathbf{h} \rangle$ is the *index of primitivity* of $\mathbf{h}$. In the sequel, when we speak of a 'multiple of a primitive vector', it is to be understood that we mean a nonzero integer multiple of a primitive vector. If $\mathbf{h} = c\mathbf{p}$ is a multiple of primitive vector $\mathbf{p}$, then, since the entries of a primitive vector must be relatively prime, c is, up to sign, the GCD of the entries of $\mathbf{h}$, and is the index of primitivity of $\mathbf{h}$.

Proposition 4 *Let $\mathbf{h}$ be a t-vector based on a set X with at least t isolated vertices. Then $\mathbf{h}$ is a multiple of a primitive vector.*

Proof. Let γ be the index of primitivity of $\mathbf{h}$. Let $b_1, \ldots, b_t$ be isolated vertices, $A = \{a_1, \ldots, a_t\}$ any t-subset disjoint from $\{b_1, \ldots, b_t\}$, and P the pairing with pairs (a_i, b_i). Then $\langle \mathbf{h}, \mathbf{f}_P \rangle = \mathbf{h}(A)$. Thus γ divides $\mathbf{h}$, and, of course, $(1/\gamma)\mathbf{h}$ is primitive. □

Proposition 5 *Let $\mathbf{h}$ be a t-vector with $t-1$ isolated vertices and let γ be the index of primitivity of $\mathbf{h}$. Then the restriction of $\mathbf{h}$ to the t-subsets of the remaining vertices is constant modulo γ.*

Proof. Let $b_1, \ldots, b_{t-1}$ be isolated vertices. Consider two t-subsets $A_1 = \{a_1, \ldots, a_{t-1}, c\}$ and $A_2 = \{a_1, \ldots, a_{t-1}, d\}$ with $t-1$ points in common, both disjoint from $B = \{b_1, \ldots, b_{t-1}\}$. Let P be the pairing with pairs (a_i, b_i), $i = 1, \ldots, t-1$, and (c, d). Then γ divides $\langle \mathbf{h}, \mathbf{f}_P \rangle = \mathbf{h}(A_1) - \mathbf{h}(A_2)$, i.e. $\mathbf{h}(A_1) \equiv \mathbf{h}(A_2) \pmod{\gamma}$. Given any two t-subsets A, A' disjoint from B, there exists a sequence $A = A_1, A_2, \ldots, A_m = A'$ of t-subsets disjoint from B so that $|A_i \cap A_{i+1}| = t-1$; hence $\mathbf{h}(A) \equiv \mathbf{h}(A') \pmod{\gamma}$. □

Theorem 6 *Let γ be the index of primitivity of a t-vector $\mathbf{h}$. Then $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ contains $\gamma\mathbf{g}$ for every integral vector $\mathbf{g}$ in the null space of $W_{t-1,t}$.*

Proof. It suffices to show that $\gamma\mathbf{f}_P$ is in $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ for every pairing P. Let P be a fixed pairing, as in (2).

For a subset $I \subseteq \{1, 2, \ldots, t\}$, let σ_I be the product of the transpositions (a_i, b_i), $i \in I$. Let $\mathbf{h}'$ be a column in $N_t(\mathbf{h})$. We claim that for each t-subset T,

$$\sum_{I \subseteq \{1,2,\ldots,t\}} \mathrm{sign}(\sigma_I) \cdot \mathbf{h}'(\sigma_I(T)) = \langle \mathbf{f}_P, \mathbf{h}' \rangle \cdot \mathbf{f}_P(T). \tag{3}$$

If T is not transverse to the pairing P, then the R.H.S. of (3) is 0. In this case, there exists i such that neither a_i nor b_i is in T, implying that $\sigma_I(T) = \sigma_{I \oplus \{i\}}(T)$ for any $I \subseteq \{1, 2, \ldots, t\}$, where $I \oplus \{i\}$ denotes the symmetric difference between I and $\{i\}$. Of course, $\mathrm{sign}(\sigma_I) = -\mathrm{sign}(\sigma_{I \oplus \{i\}})$. This means that the subsets I in (3) can be paired up as $\{I, I \oplus \{i\}\}$ so that the corresponding summands on the L.H.S. have the same magnitudes but opposite signs, and therefore the L.H.S. is also 0.

If T is transverse to the pairing P, then there is a bijection between subsets $I \subseteq \{1, 2, \ldots, t\}$ and transversals T_I to P such that $\sigma_I(T) = T_I$, and

$$\mathrm{sign}(\sigma_I) \cdot \mathbf{h}'(\sigma_I(T)) = (-1)^{|T \cap B|}(-1)^{|T_I \cap B|} \cdot \mathbf{h}'(T_I) = \mathbf{f}_P(T)\, \mathbf{f}_P(T_I)\, \mathbf{h}'(T_I),$$

where $B = \{b_1, b_2, \ldots, b_t\}$. Summing over $I \subseteq \{1, 2, \ldots, t\}$, we get (3). Now, $\langle \mathbf{f}_p, \mathbf{h}' \rangle \cdot \mathbf{f}_P$ is in $\mathrm{col}_{\mathbb{Z}}(N_t(\mathbf{h}))$ for every column $\mathbf{h}'$ in $N_t(\mathbf{h})$, then so is $\gamma\mathbf{f}_P$. □

4 Fronts and shadows

Given an $r \times s$ matrix A, $r \leq s$, a unimodular matrix E so that $EA = DB$ where D is square diagonal and B is row-unimodular will be called a *front* for A. The front E determines D uniquely, because the diagonal entry d_i of D must be the GCD of the entries of $\mathbf{e}_i A$, where $\mathbf{e}_i$ is the i-th row of E. The rows of B corresponding to nonzero diagonal entries d_i are also uniquely determined as $(1/d_i)\mathbf{e}_i A$ (while the rows corresponding to any 0's on the diagonal of D are arbitrary except subject to the constraint that B is row-unimodular). If F is the inverse of any unimodular extension of B, then $EAF = [D, O]$ is a diagonal form for A. The diagonal entries of D will be called the diagonal factors *corresponding* to the front E.

We use $A \sqcup B$ to denote a matrix obtained by placing A on top of B. Let $Y_{0t} = W_{0t}$, a $1 \times \binom{n}{t}$ matrix of all ones. For $i = 1, 2, \ldots, t$, let $Y_{it} = Y_{it}(n)$ be

the $\binom{n}{i} - \binom{n}{i-1}$ by $\binom{n}{t}$ matrix obtained from $W_{it} = W_{it}(n)$ by deleting those rows corresponding to an $(i-1,i)$-basis on $\{1,2,\ldots,n\}$. Here an $(i-1,i)$-basis is a set of i-subsets so that the corresponding columns of $W_{i-1,i}$ form a $\mathbb{Z}$-basis for $\mathrm{col}_{\mathbb{Z}}(W_{i-1,i})$; such bases exist by Proposition 1 of [11] and here we choose and fix one for each i. The following lemma is proved in [11] for $n \geq 2t$ but is easily extended to $n \geq t+i$; see [10].

Lemma 7 *Let $i \leq t \leq n-i$ be given.* (i) *The matrix*

$$\bigsqcup_{i=0}^{j} Y_{it} = \begin{array}{|c|}\hline Y_{0t} \\ \hline Y_{1t} \\ \hline Y_{2t} \\ \hline \vdots \\ \hline Y_{jt} \\ \hline \end{array}$$

is an $\binom{n}{j} \times \binom{n}{t}$ row-unimodular matrix whose rows form a $\mathbb{Z}$-basis for the integer vectors in $\mathrm{row}_{\mathbb{Q}}(W_{jt})$. (ii) *For each $j = 0,1,2,\ldots,t$, the module $\mathrm{row}_{\mathbb{Z}}(W_{jt})$ generated by the rows of W_{jt} is equal to that generated by the rows of*

$$\bigsqcup_{i=0}^{j} \binom{t-i}{j-i} Y_{it}.$$

In particular, since $W_{tt} = I$, if $n \geq 2t$, then $\sqcup_{i=0}^{t} Y_{it}$ is an $\binom{n}{t} \times \binom{n}{t}$ unimodular matrix.

For later use, we note that

$$W_{ij} W_{jt} = \binom{t-i}{j-i} W_{it}, \tag{4}$$

and, when we delete the rows corresponding to an $(i-1,i)$-basis from both sides of (4), we obtain

$$Y_{ij} W_{jt} = \binom{t-i}{j-i} Y_{it}. \tag{5}$$

Theorem 8 *Given any t-vector $\mathbf{h}$, let γ be the index of primitivity of $\mathbf{h}$. Let $U_{t-1,t}$ be any matrix whose rows form a $\mathbb{Z}$-basis for the module of integer vectors in* $\mathrm{row}_{\mathbb{Q}}(W_{t-1,t})$.

(i) *If $\gamma \neq 0$, then*

$$\tau(N_t) \quad \textit{divides} \quad \gamma^{\binom{n}{t}-\binom{n}{t-1}}\tau(U_{t-1,t}N_t) \tag{6}$$

and

$$\mathrm{rank}(N_t) = \mathrm{rank}(U_{t-1,t}N_t) \quad + \quad \binom{n}{t} - \binom{n}{t-1}. \tag{7}$$

(ii) *If $\mathbf{h}$ is a multiple of a primitive t-vector, then equality holds in* (6). *More strongly, a front for $N_t(\mathbf{h})$ can be obtained as any unimodular extension of $EU_{t-1,t}$ where E is a front for $U_{t-1,t}N_t$, and diagonal factors for N_t can be obtained by adjoining $\binom{n}{t} - \binom{n}{t-1}$ copies of γ to diagonal factors for $U_{t-1,t}N_t$.*

Proof. By Theorem 6, $\mathrm{col}_{\mathbb{Z}}(N_t)$ contains $\gamma\mathbf{v}$ for any t-pod $\mathbf{v}$. Thus the column module $\mathrm{col}_{\mathbb{Z}}(N_t)$ of N_t is equal to the column module of the matrix

$$\overline{N}_t = \left[\begin{array}{c|c} N_t & \gamma M_{t-1,t}^{\top} \end{array}\right],$$

where $M_{t-1,t}$ is any $\binom{n}{t} - \binom{n}{t-1}$ by $\binom{n}{t}$ matrix whose rows form a $\mathbb{Z}$-basis for the null module $\mathrm{null}_{\mathbb{Z}}(W_{t-1,t})$ of integer vectors orthogonal to the rows of $W_{t-1,t}$. (So the rows of $M_{t-1,t}$ may be chosen as t-pods.) Let

$$U = \left[\begin{array}{c} U_{t-1,t} \\ \hline V \end{array}\right]$$

be a unimodular extension of $U_{t-1,t}$; then

$$UM_{t-1,t}^{\top} = \left[\begin{array}{c} U_{t-1,t} \\ \hline V \end{array}\right] \left[\begin{array}{c} \\ M_{t-1,t}^{\top} \\ \\ \end{array}\right] = \left[\begin{array}{c} O \\ \hline Y \end{array}\right]$$

where the matrix Y is square of order $\binom{n}{t} - \binom{n}{t-1}$. Since $M_{t-1,t}$ is row-unimodular, Y is unimodular and $\det(Y) = \pm 1$. Then

$$U\overline{N}_t = \begin{array}{|c|c|} \hline U_{t-1,t}N_t & O \\ \hline VN_t & \gamma Y \\ \hline \end{array}. \tag{8}$$

It is clear now that the rank of N_t is the rank of $U_{t-1,t}N_t$ plus $\binom{n}{t} - \binom{n}{t-1}$. For any square submatrix X of $U_{t-1,t}N_t$ of order $\ell = \operatorname{rank}(U_{t-1,t}N_t)$, the determinant of the square submatrix of $U\overline{N}_t$ of the form

$$\begin{array}{|c|c|} \hline X & O \\ \hline Z & \gamma Y \\ \hline \end{array}$$

(where Z is a submatrix of VN_t) is a multiple of $\tau(U\overline{N}_t) = \tau(N_t)$. That is, $\tau(N_t)$ divides $\gamma^{\binom{n}{t}-\binom{n}{t-1}} \det(X)$. This implies (6).

Now assume $\mathbf{h}$ is a multiple of a primitive vector. Then the index of primitivity γ is the GCD of the entries of $\mathbf{h}$ and divides all entries of N_t. In this case, column operations can be used to transform the matrix in (8) to

$$U\overline{N}_tF_1 = \begin{array}{|c|c|} \hline U_{t-1,t}N_t & O \\ \hline O & \gamma I \\ \hline \end{array}$$

(here F_1 is an appropriate unimodular matrix). If E is a front for $U_{t-1,t}N_t$ and $EU_{t-1,t}N_t = DF$ (here D is an $\binom{n}{t-1} \times n!$ diagonal matrix), then

$$\begin{array}{|c|} \hline EU_{t-1,t} \\ \hline V \\ \hline \end{array} \overline{N}_tF_1 = \begin{array}{|c|c|} \hline D & O \\ \hline O & \gamma I \\ \hline \end{array}.$$

So $EU_{t-1,t} \sqcup V$ is a front for $\overline{N}_t$ or N_t. The matrix $EU_{t-1,t} \sqcup V$ is unimodular if and only if $U_{t-1,t} \sqcup V$ is unimodular. □

Remarks. For the matrix $U_{t-1,t}$ in the above theorem, one may take $\sqcup_{i=0}^{t-1} Y_{it}$. And in the proof, one may take $V = Y_{tt}$ independent of the choice of $U_{t-1,t}$.

For an integer j, $0 \le j \le t$, the *j-th shadow* $\mathbf{h}^{(j)}$ of a t-vector $\mathbf{h}$ is the $(t-j)$-vector $W_{t-j,t}\mathbf{h}$. For example, if $\mathbf{g}$ is the characteristic 2-vector of a multigraph G, then the first shadow of $\mathbf{h}$ is the 1-vector whose coordinates give the degrees of the vertices of G, and the second shadow of G is the scalar e, the number of edges of G. Note that by (4), a shadow of a shadow is an integer multiple of a shadow. E.g. the first shadow of the degree sequence of a graph is $2e$.

Theorem 9 *If a t-vector $\mathbf{h}$ and all of its shadows are primitive or multiples of primitive vectors, then a front for $N_t(\mathbf{h})$ is given by*

$$E = \sqcup_{i=0}^{t} Y_{it}. \tag{9}$$

The corresponding diagonal factors are

$$(g_0)^1,\ (g_1)^{n-1},\ (g_2)^{\binom{n}{2}-n}, \ldots,\ (g_t)^{\binom{n}{t}-\binom{n}{t-1}}, \tag{10}$$

where g_i is the GCD *of all entries of $W_{it}\mathbf{h}$.* (*Here the exponents denote multiplicities.*)

Proof. The diagonal factors of a matrix do not change if repeated columns are deleted or allowed to remain. For the purposes of this proof, we will assume that all matrices N_i have $n!$ columns, one for each permutation. This allows us to write, for example, $N_{t-j}(\mathbf{h}^{(j)}) = W_{t-j,t}N_t(\mathbf{h})$ without worrying whether the j-th shadow has fewer distinct images under the symmetric group.

We proceed by induction on t. The theorem is trivial when $t = 0$. (A 0-vector is a multiple of a primitive vector if and only if its single entry is a nonzero integer c. The matrix N_0 is a 1 by $n!$ matrix of c's, etc.) Now fix $t \ge 1$.

Given $\mathbf{h}$, let $\mathbf{h}' = W_{t-1,t}\mathbf{h}$ be the first shadow of $\mathbf{h}$. Then $N_{t-1}(\mathbf{h}') = W_{t-1,t}N_t(\mathbf{h})$. We write N_t for $N_t(\mathbf{h})$ and N_{t-1} for $N_{t-1}(\mathbf{h}')$. Let g_i' be the GCD of the entries of $W_{i,t-1}\mathbf{h}'$ for $i = 0, 1, \ldots, t-1$. Then, by (4),

$$g_i' = (t-i)g_i, \qquad i = 0, 1, \ldots, t-1. \tag{11}$$

We may apply the induction hypothesis to $\mathbf{h}'$ and we conclude that $\sqcup_{i=0}^{t-1} Y_{i,t-1}$ is a front for N_{t-1} with corresponding diagonal form

$$D = \operatorname{diag}\big((g_i')^{\binom{n}{i}-\binom{n}{i-1}},\ i = 0, 1, \ldots, t-1\big). \tag{12}$$

By (5),

$$(\sqcup_{i=0}^{t-1} Y_{i,t-1})W_{t-1,t}N_t = (\sqcup_{i=0}^{t-1}(t-i)Y_{it})N_t = D'(\sqcup_{i=0}^{t-1} Y_{it})N_t$$

where D' is the square diagonal matrix with diagonal entries

$$(t-i)^{\binom{n}{i}-\binom{n}{i-1}},\ i=0,1,\ldots,t-1. \tag{13}$$

By (11), (12), and (13), a diagonal form for $(\sqcup_{i=0}^{t-1}Y_{it})N_t$ is

$$\operatorname{diag}\big((g_i)^{\binom{n}{i}-\binom{n}{i-1}},\ i=0,1,\ldots,t-1\big).$$

The index of primitivity γ of $\mathbf{h}$ is the GCD of the entries of $\mathbf{h}$, and this is g_t. By Theorem 8(ii), $\sqcup_{i=0}^{t}Y_{it}$ is a front for N_t with corresponding diagonal form

$$\operatorname{diag}\big((g_i)^{\binom{n}{i}-\binom{n}{i-1}},\ i=0,1,\ldots,t\big).$$

□

5 Primitivity of random hypergraphs

We consider the following model for a random t-uniform multihypergraph on k vertices. Let X_T be a random variable associated with each edge T of $K_k^{(t)}$, and assume the X_T's are i.i.d. and uniformly distributed on $\{0,1,\ldots,M-1\}$ for some $M\geq 2$. Let H be the 'random multihypergraph' where the multiplicity of each edge T is given by X_T.

Let $P=\{(a_1,b_1),(a_2,b_2),\ldots,(a_t,b_t)\}$ be a pairing, σ_I the product of the transpositions (a_i,b_i), $i\in I\subseteq\{1,2,\ldots,t\}$. Let $T=\{a_1,a_2,\ldots,a_t\}$. By definition, H is primitive if and only if the GCD of

$$\sum_{I\subseteq\{1,2,\ldots,t\}}(-1)^{|I|}X_{\sigma_I(T)}$$

with P running over all pairings in the k-set is 1. Note that if we fix a pairing P, for any prime p,

$$\mathbb{P}\left(\sum_{I\subseteq\{1,2,\ldots,t\}}(-1)^{|I|}X_{\sigma_I(T)}\equiv_p 0\right)=\ \mathbb{P}\left(\sum_{i=1}^{2^{t-1}}X_{T_i}-\sum_{i=1}^{2^{t-1}}X_{T_i'}\equiv_p 0\right)$$

$$=\sum_{r=-(M-1)(2^{t-1}-1)}^{(M-1)2^{t-1}}\mathbb{P}\left(\sum_{i=1}^{2^{t-1}}X_{T_i}-\sum_{i=2}^{2^{t-1}}X_{T_i'}=r\right)\cdot\mathbb{P}\left(X_{T_1'}\equiv_p r\right)\leq\frac{1}{M}\left\lceil\frac{M}{p}\right\rceil,$$

since $\mathbb{P}\left(X_{T_1'}\equiv_p r\right)=\frac{1}{M}\left\lfloor\frac{M}{p}\right\rfloor$ or $\frac{1}{M}\left\lceil\frac{M}{p}\right\rceil$ for all $r\in\mathbb{Z}$.

If we form $\lfloor k/2t \rfloor$ disjoint subsets of $2t$ vertices out of the set of k vertices, and from each subset of $2t$ vertices we choose a pairing, then

$$\begin{aligned}\mathbb{P}(H \text{ is non-primitive}) &\leq \sum_{p \text{ prime} \leq (M-1)2^{t-1}} \left(\frac{1}{M} \left\lceil \frac{M}{p} \right\rceil \right)^{\lfloor k/2t \rfloor} \\ &\leq (M-1)2^{t-1} \, (2/3)^{\lfloor k/2t \rfloor} \xrightarrow{k \to \infty} 0,\end{aligned}$$

which proves the following theorem.

Theorem 10 *A random t-uniform multihypergraph H on k vertices is almost surely primitive as $k \to \infty$.*

We remark that the i-th shadow of a random t-uniform hypergraph is not necessarily a random $(t-i)$-uniform hypergraph, yet we show that it, too, is almost surely primitive.

Consider the i-th shadow $H^{(i)}$ of H. For each edge $R = \{a_1, \ldots, a_{t-i}\}$ in $H^{(i)}$, let $Z_R = \sum_{T \in E(H) \text{ s.t. } R \subset T} X_T$, which represents the multiplicity of each edge R in $H^{(i)}$. Then $H^{(i)}$ is primitive if and only if the GCD of

$$\omega(P^{(i)}) := \sum_{I \subseteq \{1,2,\ldots,t-i\}} (-1)^{|I|} Z_{\sigma_I(\{a_1,a_2\ldots,a_{t-i}\})}$$

with $P^{(i)} = \{(a_1, b_1), (a_2, b_2), \ldots, (a_{t-i}, b_{t-i})\}$ running over all pairings in the k-set is 1.

We form $\lfloor k/2(t-i) \rfloor$ disjoint subsets of $2(t-i)$ vertices out of the set of k vertices, and from each subset of $2(t-i)$ vertices we choose a pairing, labeled by $P_1^{(i)}, P_2^{(i)}, \ldots, P_{\lfloor k/2(t-i) \rfloor}^{(i)}$. For each pairing $P_j^{(i)}$, since $k \to \infty$, there always exists at least one t-subset T such that X_T occurs only once in $\omega(P_j^{(i)})$ but not in any other $\omega(P_\ell^{(i)})$. Hence, the independence of the X_T's gives

$$\mathbb{P}(H^{(i)} \text{ is non-primitive}) \leq \sum_{p \text{ prime} \leq (M-1)2^{t-i-1}\binom{k-2(t-i)}{i}} \left(\frac{1}{M} \left\lceil \frac{M}{p} \right\rceil \right)^{\lfloor k/2(t-i) \rfloor},$$

which also goes to 0 when $k \to \infty$, and so we obtain the following theorem.

Theorem 11 *The i-th shadow $H^{(i)}$ of a random multi-hypergraph H on k vertices is almost surely primitive as $k \to \infty$.*

In fact, both theorems hold for any distribution of i.i.d. random variables X_T as long as $\mathbb{P}(X_T \equiv_p r) < 1$ for all primes p and $r \in \mathbb{Z}$. Finally, note that when $M = 2$, our original setting coincides with one of the most classical definition of random hypergraph.

6 Fronts and diagonal forms for primitive 2-vectors and graphs

For a 1-vector $\mathbf{a} = (a_1, \ldots, a_n)$, $N_1(\mathbf{a})$ has as columns all permutations of $\mathbf{a}$. Let $B = B(b; a_1, \ldots, a_n)$ be the matrix obtained from $N_1(\mathbf{a})$ by replacing the top row by $(b, b, \ldots, b)$ for some integer b.

Theorem 12 *Given integers $a_1, \ldots, a_n$ and b, not all zero, let*

$$h = \mathrm{GCD}\{a_1, \ldots, a_n, b\} \qquad \textit{and} \qquad g = \mathrm{GCD}_{1 \le i,j \le n}(a_i - a_j).$$

If $b \neq 0$, a front for $B(b; a_1, \ldots, a_n)$ is the matrix

$$E = \begin{pmatrix} (a_1, g)/h & \ell b/h & 0 & 0 & \ldots & 0 \\ u & v & 0 & 0 & \ldots & 0 \\ 0 & -1 & 1 & 0 & \ldots & 0 \\ 0 & -1 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \ddots & \vdots \\ 0 & -1 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

and the corresponding diagonal factors are

$$(bg/h)^1,\ (h)^1,\ (g)^{n-2}.$$

Here, ℓ is any integer relatively prime to a_1/h and g/h such that $(a_1, g) + \ell a_1 \equiv 0 \pmod{g}$, and u, v are chosen so that

$$\det \begin{pmatrix} (a_1, g)/h & \ell b/h \\ u & v \end{pmatrix} = 1.$$

If $b = 0$, the front E should be modified by replacing the first two rows of E with $(1, 0, 0, \ldots, 0)$ and $(0, 1, 0, \ldots, 0)$ respectively; the corresponding diagonal factors are as above, with bg/h replaced by 0.

Remarks. If $g = 0$, i.e. $a_1 = a_2 = \cdots = a_n$, then all columns of B are the same. But we should understand that this column is to be repeated so that B has at least n columns and our definition of front can be applied as stated.

Proof. We omit the simple details for the case $b = 0$. We prove the theorem when $h = 1$, and the full result follows.

Given $i, j, k,\ k \geq 2$, we can find two columns of B that agree in all coordinates except the k-th, where one contains a_i and the other a_j. For example, if $i = 1$, $j = 2$, $k = 3$, the columns could be

$$[b, a_3, a_1, a_4, a_5, \ldots, a_n]^\top \qquad \text{and} \qquad [b, a_3, a_2, a_4, a_5, \ldots, a_n]^\top.$$

Then $\mathrm{col}_{\mathbb{Z}}(B)$ contains their difference, the vector $(a_i - a_j)\mathbf{u}_k$ where $\mathbf{u}_k$ is the k-th standard basis vector. It follows that for each $k \geq 2$, $\mathrm{col}_{\mathbb{Z}}(B)$ contains the vector $g\mathbf{u}_k$. It can then be seen that the matrix

$$C = \begin{pmatrix} b & 0 & 0 & \ldots & 0 \\ a_1 & g & 0 & \ldots & 0 \\ a_1 & 0 & g & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ a_1 & 0 & 0 & \ldots & g \end{pmatrix}$$

has the same column module as B, and hence the same fronts and diagonal factors.

For $b \neq 0$, it is easy to check that integers ℓ with the stated properties exist and that E is unimodular. Also, $EC = DU$, where $D = \mathrm{diag}((bg)^1, (1)^1, (g)^{n-2})$ and U is (square and) integral. The only non-trivial instance to be checked is that $\mathbf{e}C \equiv 0 \pmod{bg}$ where $\mathbf{e}$ is the top row of E. This is

$$\mathbf{e}C = (a_1, g)(b, 0, 0, \ldots, 0) + \ell b(a_1, g, 0, \ldots, 0).$$

The first coordinate $b\big((a_1, g) + \ell a_1\big)$ is divisible by bg by our choice of ℓ, and all other coordinates are obviously divisible by bg.

Finally, note that $\det(C) = \det(D)$, and when this is nonzero, $\det(U) = \det(E)$; that is, U is unimodular and the proof is complete. If $\det(C) = 0$, i.e. $g = 0$, then $\ell = -1$, $a_1 v + bu = 1$, and EC is the matrix with all rows $\mathbf{0}$ except that the second row is $\mathbb{1}$. Then $EC = DU'$ where U' is any unimodular matrix with second row $\mathbb{1}$. □

Note that this theorem describes diagonal forms for $N_1(\mathbf{a})$ for any nonzero $\mathbf{a}$ when we replace b by $a_1 + a_2 + \cdots + a_n$, since in that case $\mathrm{row}_{\mathbb{Z}}(N_1(\mathbf{a})) = \mathrm{row}_{\mathbb{Z}}(B)$. We now describe a front and diagonal factors for $N_2(\mathbf{h})$ for any primitive 2-vector $\mathbf{h}$.

Theorem 13 *Let* $\mathbf{h}$ *be a primitive* 2*-vector based on an* n*-set with first shadow* $\mathbf{a} = [a_1, \ldots, a_n]^\top$*. Let* $b = (a_1 + \cdots + a_n)/2$ *and let* g, h, E *be described as in the statement of Theorem* 12*. As a front for* $N_2(\mathbf{h})$ *we may take* $(E(Y_{02} \sqcup Y_{12})) \sqcup Y_{22}$*, and the corresponding diagonal factors are*

$$(bg/h)^1,\ (h)^1,\ (g)^{n-2},\ (1)^{\binom{n}{2}-n}.$$

Proof. We use the matrix $U_{12} = Y_{02} \sqcup Y_{12}$ in Theorem 8(ii). We have $W_{12}N_2 = N_1((a_1, \ldots, a_n))$ and $W_{02}N_2 = (b, b, \ldots, b)$. Since Y_{02} is a row of all 1's and Y_{12} is W_{12} with the top row, say, deleted, $(Y_{02} \sqcup Y_{12})N_2$ has the form $B(b; a_2, \ldots, a_n)$. Theorem 8(ii) completes the proof. □

Remarks. If $\mathbf{h}$ is the characteristic 2-vector of a multigraph G, then the shadow $\mathbf{a} = W_{12}\mathbf{h}$ is the degree sequence of G and b is the number of edges of G; in particular, diagonal factors of a primitive multigraph are determined by its degree sequence. A multigraph is regular if and only if $g = 0$. As simple examples, diagonal factors for $N_2(G)$ where G is the Petersen graph ($n = 10$) are $(3)^1$, $(0)^9$, $(1)^{35}$, while for the graph G' ($n = 11$) consisting of the Petersen graph plus an isolated vertex, diagonal factors of $N_2(G')$ are $(15)^1$, $(3)^{10}$, $(1)^{44}$. The Petersen graph (and almost every simple graph) is primitive by Theorem 14 in the next section.

The problem of describing diagonal factors for N_2 for all 2-vectors or multigraphs seems very difficult. But we are able to describe them for $N_2(G)$ for all simple graphs.

7 Fronts and diagonal factors for non-primitive simple graphs

We use $\mathbf{1}_{\{x,y\}}$ to denote a row vector of length $\binom{k}{2}$, indexed by the 2-subsets of V, such that the entry corresponding to $\{x, y\}$ is 1 and 0 elsewhere. Then the 2-pod corresponding to the pairing $P = \{(a_1, b_1), (a_2, b_2)\}$ has the form

$$\mathbf{f}_P = \mathbf{1}_{\{a_1,a_2\}} + \mathbf{1}_{\{b_1,b_2\}} - \mathbf{1}_{\{a_1,b_2\}} - \mathbf{1}_{\{a_2,b_1\}}.$$

If G is a simple graph with characteristic 2-vector $\mathbf{g}$, then

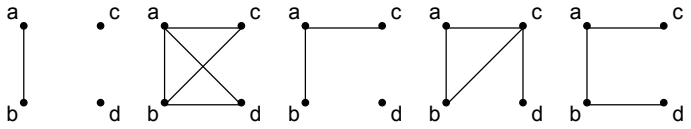
$$\langle \mathbf{f}_P, \mathbf{g} \rangle = \mathbf{g}(\{a_1, a_2\}) + \mathbf{g}(\{b_1, b_2\}) - \mathbf{g}(\{a_1, b_2\}) - \mathbf{g}(\{a_2, b_1\}),$$

where, of course, $\mathbf{g}(\{x, y\}) = 1$ if $\{x, y\}$ is an edge of G and $\mathbf{g}(\{x, y\}) = 0$ otherwise. So we always have $\langle \mathbf{f}_p, \mathbf{g} \rangle \in \{-2, -1, 0, 1, 2\}$.

Theorem 14 *A simple graph G with at least four vertices is primitive unless G is isomorphic to a complete graph, an edgeless graph, a complete bipartite graph, or a disjoint union of two complete graphs.*

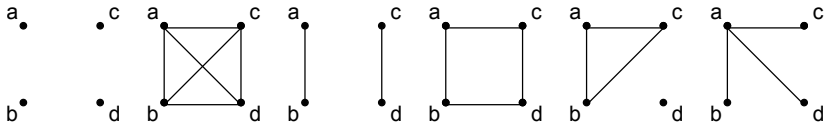
Proof. It is easy to check which simple graphs on four vertices are primitive. (Up to sign, there are only three 2-pods.) These are the primitive simple

graphs on four vertices. (For example, if G is the fourth graph and $P = \{(a,c),(d,b)\}$, then $\langle \mathbf{f}_P, \mathbf{g} \rangle = -1$.)



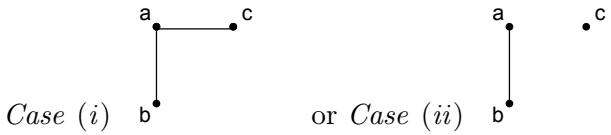
(14)

Hence G is non-primitive if and only if every subgraph induced by four vertices of G is isomorphic to one of the following.

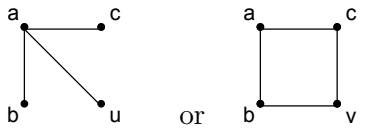


Note that a simple graph is primitive if and only if its complement is primitive.

Now, assume that G is non-primitive. If G is not a complete graph or an edgeless graph, then there exist three vertices a, b, c such that the subgraph they induce is isomorphic to



Case (i). For every vertex $x \neq a, b, c$ in G, the induced subgraph on $\{a, b, c, x\}$ is isomorphic to



Let U and V be, respectively, the sets of vertices other than a, b, c that are adjacent to a, and are adjacent to b and c. Observe that two vertices $u_1, u_2 \in U$ cannot be adjacent in G, or else the subgraph induced by $\{a, b, u_1, u_2\}$ is on the list (14); two vertices $v_1, v_2 \in V$ cannot be adjacent in G, or else the subgraph induced by $\{a, b, v_1, v_2\}$ is on the list (14); and vertices $u \in U$, $v \in V$ must be adjacent in G, or else the subgraph induced by $\{a, b, u, v\}$ is on the list (14). Therefore, G is a complete bipartite graph with parts $\{b, c\} \cup U$ and $\{a\} \cup V$.

In *Case* (ii), the complement of the graph falls under Case (i). □

The following theorems give diagonal factors for non-primitive simple graphs.

We omit any discussion of edgeless and complete graphs. The graphs $K_{1,k-1}$ and $K_1 \dot\cup K_{k-1}$ have index of primitivity 0. Explicit fronts for these graphs are given in [13]. We do not require these fronts in Section 9 and give only the simple diagonal factors here.

Theorem 15 *Diagonal factors for $N_2(G)$ when $G = K_{1,k-1}$ are*

$$(2)^1,\ (1)^{k-1},\ (0)^{\binom{k}{2}-k}.$$

Proof. It is easy to see that $N_2(K_{1,k-1})$ (using only the k distinct subgraphs as columns) has as rows all vectors with two 1's and $k-2$ 0's. That is, $N_2(K_{1,k-1}) = (N_1(\mathbf{a}))^\top$ where $\mathbf{a}$ is a column vector $[1,1,0,\ldots,0]^\top$. Then $N_2(K_{1,k-1})$ and $N_1(\mathbf{a})$ have the same diagonal forms, apart from trailing 0's. By Theorem 12, diagonal factors for $N_1(\mathbf{a})$ are $(2)^1,\ (1)^{k-1}$. □

Theorem 16 *Diagonal factors for $N_2(G)$ when $G = K_1 \dot\cup K_{k-1}$ are*

$$(k-2)^1,\ (1)^{k-1},\ (0)^{\binom{k}{2}-k}.$$

Proof. It is easy to see that $N_2(K_1 \dot\cup K_{k-1})$ has as rows all vectors with two 0's and $k-2$ 1's. That is, $N_2(K_{1,k-1}) = (N_1(\mathbf{a}))^\top$ where $\mathbf{a} = [0,0,1,\ldots,1]^\top$. By Theorem 12, diagonal factors for $N_1(\mathbf{a})$ are $(k-2)^1,\ (1)^{k-1}$, and the result follows. □

The graphs $K_{r,k-r}$ and $K_r \dot\cup K_{k-r}$ with $2 \le r \le k-2$ have index of primitivity 2. The proofs of the next two theorems use Theorem 12(i) and Lemma 1. We are brief in the proof of the first theorem and just sketch the proof of the second. Full details may be found in [13].

Theorem 17 *If $G = K_{r,k-r}$, $2 \le r \le k-2$, then a front for $N_2(G)$ is given by the matrix E shown below*

$(1\ 1\ \cdots\ 1) + \ell e/h \times$ *second row of* W_{12}	} 1 *row*
second row of W_{12}	} 1 *row*
$\sum_{i=1}^{k-3} \left(\mathbf{1}_{\{w_i,x\}} - \mathbf{1}_{\{w_i,y\}}\right) - (k-2r-1)\left(\mathbf{1}_{\{x,z\}} - \mathbf{1}_{\{y,z\}}\right)$, x / y / z: v_2 / v_{k-1} / v_k; v_3 / v_{k-1} / v_k; $\vdots$ / $\vdots$ / $\vdots$; v_{k-2} / v_{k-1} / v_k; v_{k-2} / v_k / v_{k-1} *and* $\{w_i\}_{i=1}^{k-3} = V\backslash\{x,y,z\}$	} $k-2$ *rows*
$\mathbf{1}_{\{x,y\}} + \mathbf{1}_{\{x,v_k\}} + \mathbf{1}_{\{y,v_k\}}$, $\{x,y\} \subseteq \{v_2,\ldots,v_{k-1}\}$ *except* $\{x,y\} = \{v_2,v_3\}$	} $\binom{k-2}{2} - 1$ *rows*
$\mathbf{1}_{\{x,v_k\}}$, $x \in \{v_2,\ldots,v_{k-1}\}$	} $k-2$ *rows*

where ℓ *is an integer such that* $1 + \ell r/h \equiv 0 \pmod{g/h}$*, and the corresponding diagonal factors for* $N_2(G)$ *are*

$$(eg/h)^1,\ (h)^1,\ (2g)^{k-2},\ (2)^{\binom{k}{2}-(2k-2)},\ (1)^{k-2},$$

where $e = r(k-r)$*,* $g = k-2r$*, and* $h = \mathrm{GCD}(r,k)$*.*

Proof. We only focus on the case where $k \neq 2r$, and leave the case where $k = 2r$ to [13].

Consider first $U_{12}N_2(K_{r,k-r})$, where $U_{12} = Y_{02} \sqcup Y_{12}$. In the notation of Theorem 12, this matrix is $B(e;\delta_1,\delta_2,\ldots,\delta_k)$ where e is the number of edges and the δ_i's are the degrees of $K_{r,k-r}$, i.e. each δ_i is r or $k-r$. Theorem 12 gives diagonal factors for $U_{12}N_2$ in terms of e and the parameters g and h as defined in the statement of that theorem, and these parameters are now expressed in terms of k and r in Theorem 17. Note that $g \neq 0$ if and only $k \neq 2r$.

In particular, when $k \neq 2r$, a consequence of Theorem 12 is

$$\tau(U_{12}N_2) = eg^{k-1}, \qquad \mathrm{rank}(U_{12}N_2) = k.$$

By Theorem 8, we have

$$\tau(N_2) \mid 2^{\binom{k}{2}-k} e g^{k-1}, \qquad \operatorname{rank}(N_2) = \tbinom{k}{2}.$$

Let E and D be as described in the statement of the theorem. We claim that E is unimodular and that $EN_2 = DC$ where C is an integer matrix. Since

$$\tau(D) = 2^{\binom{k}{2}-k} e g^{k-1}, \qquad \operatorname{rank}(D) = \tbinom{k}{2},$$

Lemma 1 will complete the proof.

(It is perhaps curious, here and in Theorem 18, how the powers of 2 interact with diagonal factors of $U_{12}N_2$ to produce diagonal factors for N_2 itself. It was not evident what to use for E and D without a good deal of computer experimentation.)

If the 2-subsets that index the columns of E are ordered lexicographically, then E has the form

A	B
O	C

where $A =$

$$\begin{pmatrix}
1+\ell e/h & 1 & 1 & \cdots & 1 & 1 & 1 & 1+\ell e/h \\
1 & & & & & & & 1 \\
1 & & & & & -1 & & 1 \\
 & & 1 & & & -1 & & 1 \\
 & & & 1 & & -1 & & \\
 & & & & \ddots & \vdots & & \\
 & & & & & 1 & -1 & \\
 & & & & & 1 & & -1
\end{pmatrix}$$

Here A is square of order k and C is square of order $\binom{k}{2} - k$. Elementary $\mathbb{Z}$-row operations show that $\det(A) = \pm 1$. It can be seen that the leading entries of the rows of C are 1's and that these leading entries are in different columns. That is, row permutations will take C to an upper triangular matrix with 1's on the diagonal. It is now clear that E is unimodular.

The first row of EN_2 is

$$\mathbb{1}N_2 + (\ell e/h)(\text{second row of } W_{12}) \times N_2 = e\mathbb{1} + (\ell e/h)\mathbf{v}$$

where $\mathbf{v}$ is a vector with entries r and $k - r$. So the entries of the first row of EN_2 are either $e(1 + \ell r)/h$ or $e(1 + \ell(k - r))/h$, and both are divisible by eg/h by the definition of ℓ.

The second row of EN_2 has entries r and $k-r$, both of which are divisible by h.

Let x, y, z be distinct vertices and consider the entry in column G_0, where G_0 is isomorphic to $K_{r,k-r}$, of

$$\left(\sum_{w \neq x,y,z} \left(\mathbf{1}_{\{w,x\}} - \mathbf{1}_{\{w,y\}} \right) - (k - 2r - 1) \left(\mathbf{1}_{\{x,z\}} - \mathbf{1}_{\{y,z\}} \right) \right) N_2.$$

This is 0 if x, y are not adjacent in G_0 and 0 or $\pm 2g$ if x, y are adjacent in G_0, depending on which partite set x, y and z lie in. Thus the entries in rows 3 through k of EN_2 are divisible by $2g$.

The next $\binom{k-2}{2} - 1$ rows of $EN_2(G)$ have entries 0 or 2 since any three vertices contain 0 or 2 edges of a complete bipartite graph.

Of course, the last $k-2$ rows of $EN_2(G)$ have entries divisible by 1. $\square$

We note that diagonal factors for $N_2(K_{2,k-2})$, which is the adjacency matrix of the complement of the line graph of K_n, was given by Brouwer and Van Eijl [2] in 1992.

Theorem 18 (i) *If $G = K_r \dot{\cup} K_{k-r}$, $r \leq 2 \leq k-2$ and k is odd, then a front is given by*

<table>
<tr><td>$(1\ 1\ \cdots\ 1) + \ell e/h \times$ second row of W_{12}
$+eg/h \times (0\ 0\ \cdots\ 0\ 1\ 1\ 1)$</td><td>} 1 row</td></tr>
<tr><td>second row of W_{12}</td><td>} 1 row</td></tr>
<tr><td>$\sum_{i=1}^{k-3} \left(\mathbf{1}_{\{w_i,x\}} - \mathbf{1}_{\{w_i,y\}}\right) - (k-2r-1)\left(\mathbf{1}_{\{x,z\}} - \mathbf{1}_{\{y,z\}}\right)$,
<table>
<tr><th>x</th><th>y</th><th>z</th></tr>
<tr><td>v_2</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_3</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td></tr>
<tr><td>v_{k-2}</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_{k-2}</td><td>v_k</td><td>v_{k-1}</td></tr>
</table>
and $\{w_i\}_{i=1}^{k-3} = V\backslash\{x,y,z\}$</td><td>} $k-2$ rows</td></tr>
<tr><td>$\mathbf{1}_{\{w,x\}} + \mathbf{1}_{\{w,y\}} + \mathbf{1}_{\{x,z\}} + \mathbf{1}_{\{y,z\}}$,
<table>
<tr><th>w</th><th>x</th><th>y</th><th>z</th></tr>
<tr><td>v_2</td><td>v_4</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td></tr>
<tr><td>v_2</td><td>v_{k-2}</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_2</td><td>v_{k-1}</td><td>v_k</td><td>v_3</td></tr>
<tr><td>v_3</td><td>v_4</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td></tr>
<tr><td>v_3</td><td>v_{k-2}</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_3</td><td>v_{k-1}</td><td>v_k</td><td>v_4</td></tr>
<tr><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td><td>$\vdots$</td></tr>
<tr><td>v_{k-4}</td><td>v_{k-3}</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_{k-4}</td><td>v_{k-2}</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_{k-4}</td><td>v_{k-1}</td><td>v_k</td><td>v_{k-3}</td></tr>
<tr><td>v_{k-3}</td><td>v_{k-2}</td><td>v_{k-1}</td><td>v_k</td></tr>
<tr><td>v_{k-3}</td><td>v_{k-1}</td><td>v_k</td><td>v_{k-2}</td></tr>
</table>
} $\binom{k-2}{2} - 2$ rows</td></tr>
<tr><td>$\mathbf{1}_{\{x,y\}}$,
$\{x,y\} = \{v_2,v_k\}, \{v_3,v_k\}, \ldots, \{v_{k-1},v_k\}, \{v_{k-2},v_{k-1}\}$</td><td>} $k-1$ rows</td></tr>
</table>

where ℓ is even and such that $1 + \ell(r-1)/h \equiv 0 \pmod{g/h}$, and the corresponding diagonal factors for $N_2(G)$ are

$$(2eg/h)^1,\ (h)^1,\ (2g)^{k-2},\ (2)^{\binom{k}{2}-(2k-1)},\ (1)^{k-1},$$

where $e = \binom{r}{2} + \binom{k-r}{2}$, $g = k-2r$, and $h = \mathrm{GCD}(r-1, g, e)$.
(ii) *If k is even and $r - 1 \equiv \lambda \pmod{2h}$, where $\lambda = 0$ or h, then a front can*

be given by the same matrix except the first two rows are replaced by

$(1\ 1\ \cdots\ 1) + \ell\frac{e}{h} \times$ *second row of* W_{12}	} 1 *row*
second row of $W_{12} + \lambda \times (0\ 0\ \cdots\ 0\ 1\ 1\ 1)$	} 1 *row*

where ℓ *is an integer such that* $1 + \ell(r-1)/h \equiv 0 \pmod{g/h}$*, and the corresponding diagonal factors for* $N_2(G)$ *are*

$$(eg/h)^1,\ (2h)^1,\ (2g)^{k-2},\ (2)^{\binom{k}{2}-(2k-1)},\ (1)^{k-1},$$

where $e = \binom{r}{2} + \binom{k-r}{2}$*,* $g = k - 2r$*, and* $h = \mathrm{GCD}(r-1, g, e)$*.*

Proof. As in the proof of Theorem 17, using Theorem 12(i) and Lemma 1, it will be sufficient to show, in either case k even or odd, that E is unimodular and that $EN_2 = DC$ where C is an integer matrix. Verification of this claim is mostly straightforward, though there are a number of cases. Complete details will be found in [13]. □

8 A zero-sum Ramsey-type problem of Alon and Caro

The following problem was introduced by N. Alon and Y. Caro [1] in 1993. Given a simple t-uniform hypergraph H on k vertices and an integer m which divides the number of edges of H, determine the least integer $n \geq k$ (called $R_m(H)$) so for any coloring of the t-subsets of an n-set X with the elements of $\mathbb{Z}_m$, there exists an isomorphic copy of H in the complete t-uniform hypergraph on X so that the *sum* of the colors on its edges, in $\mathbb{Z}_m$, is 0.

Equivalently, $R_m(H)$ is the smallest integer n so that the row module of $N_t(H^{\uparrow n})$ does not contain a vector with all coordinates $\not\equiv 0 \pmod{m}$. Here $H^{\uparrow n}$ is the hypergraph obtained by adjoining isolated vertices to get a total of n vertices.

Theorem 19 *Let* $\mathbf{h}$ *be a* t*-vector based on a* k*-set* X*,* $k \geq 2t$*, and suppose that* $\mathbf{h}$ *and all of its shadows are multiples of primitive vectors. Let* e *be the sum of all entries of* $\mathbf{h}$*. Then* $\mathbb{1} \in \mathrm{row}_m(N_t(\mathbf{h}))$ *if and only if* $(e, m) = 1$*.*

Proof. Let E and D be as in the statement of Theorem 9, and let F be the unimodular matrix such that $EN_tF = D$. By Lemma 2, there is an integer solution $\mathbf{y}$ to $\mathbf{y}N_t \equiv \mathbb{1} \pmod{m}$ if and only if the i-th entry of $\mathbb{1}F$ is divisible

by the GCD of m and d_i. In this case, the first row of E is $\mathbb{1}$, so the first row of EN_t is $(e, e, \ldots, e)$. As the first diagonal element of D is e, we have $\mathbb{1}F = (1, 0, \ldots, 0)$. So the system has a solution if and only if $(e, m) = 1$. □

When we take $m = 2$, we obtain the following theorems as corollaries.

Theorem 20 *If H is a t-uniform hypergraph on $k \geq 2t$ vertices with an even number of edges and such that H and all its shadows are primitive, then $R_2(H) = k$.*

Theorem 21 *If H is any t-uniform hypergraph on $k \geq 2t$ vertices with an even number of edges, then $R_2(H) \leq k + t$.*

Proof. When $n \geq k + t$, the hypergraph $H^{\uparrow n}$ and all of its shadows have at least t isolated vertices for $n \geq k + t$. The result follows from Proposition 4 and Theorem 20. □

We remark that the above was proved for $H = K_k^{(t)}$, the complete t-uniform hypergraph, by Caro [3] in 1993. The full statement above is from [12].

Theorem 22 *If H is a simple t-uniform hypergraph on $k \geq 2t$ vertices with an even number of edges that is not edgeless or complete, then $R_2(H) \leq k + t - 1$.*

Proof. When $n \geq k + t - 1$, $H^{\uparrow n}$ has at least $t - 1$ isolated vertices, and since it is simple but H is not edgeless or complete, $H^{\uparrow n}$ is primitive by Proposition 5. The j-th shadow of $H^{\uparrow n}$, $j \geq 1$, has at least $t - 1 \geq t - j$ isolated vertices and so is primitive by Proposition 4. Theorem 20 completes the proof. □

We remark that if $H = K_k^{(t)}$ is a complete t-uniform hypergraph and $\binom{k}{t}$ is even, a formula for $R_2(H)$ is given in [12] as $k + 2^e$ where 2^e is the smallest power of 2 that appears in the base 2 representation of t but not in the base 2 representation of k. So even when H is complete, $R_2(H) \leq k + t - 1$ holds except when t is a power of 2, in which case $R_2(H) = k + t$.

Theorem 23 *Let H be a simple random t-uniform hypergraph on k vertices with an even number of edges. Then $R_2(H) = k$ almost surely as $k \to \infty$.*

Proof. This follows from Theorems 10, 11, and 20. □

9 When is $\mathbb{1} \in \mathrm{row}_p(N_2(G))$ for graphs G?

The following theorem is from [4].

Theorem 24 (Y. Caro) *Let G be a simple graph with k vertices and an even number of edges. Then*

$$R_2(G) = \begin{cases} k+2 & \text{if } G \text{ is complete,} \\ k+1 & \text{if } G \text{ is the union of two complete graphs,} \\ k+1 & \text{if } G \neq K_k \text{ has all vertices of odd degree,} \\ k & \text{otherwise.} \end{cases}$$

This theorem is a corollary of Theorem 25 below (we omit the details). Caro's proof of Theorem 24 is significantly shorter than that we obtain from our viewpoint, but it is not clear whether his methods can be extended to obtain our theorem for all primes p. It is interesting to note that $p = 2$ is often a special case in the statement of Theorem 25. In Theorem 25, we opt to restrict our results for prime moduli p, rather than general moduli m, because the statements become more complex in the general case.

Theorem 25 *Let G be a simple graph with $k \geq 4$ vertices and let p be a prime divisor of the number e of edges of G. Let $\delta_1, \ldots, \delta_k$ be the degree sequence of G, g the* GCD *of all differences $\delta_i - \delta_j$, and h the* GCD *of the degrees δ_i and e. Then $\mathbb{1} \in \mathrm{row}_p(N_2(G))$ if and only if one of the following holds:*

(i) *G is primitive with $p \mid g$ but $p \nmid h$,*

(ii) *$G = K_k$,*

(iii) *$G = K_{1,k-1}$ and $p > 2$,*

(iv) *$G = K_1 \dot\cup K_{k-1}$ and $p = 2$ or $p \nmid k-2$,*

(v) *$G = K_r \dot\cup K_{k-r}$, $2 \leq r \leq k-2$, and $p = 2$ or ($p \mid g$ but $p \nmid h$).*

We will consider the case that G is primitive and the cases referenced in Theorem 14 individually. We dispense with the easy cases first. If G is edgeless, $\mathbb{1} \notin \mathrm{row}_p(N_2)$; if G is complete, $\mathbb{1} \in \mathrm{row}_p(N_2)$.

For $G = K_{1,k-1}$, as we have observed in the proof of Theorem 15, the rows of N_2 are all vectors of length k with two 1's and $k-2$ 0's. It is then easy to see that $\mathrm{row}_{\mathbb{Z}}(N_2)$ consists of all integer vectors $(a_1, \ldots, a_k)$ with $a_1 + \cdots + a_k \equiv 0 \pmod 2$. Thus $\mathbb{1} \in \mathrm{row}_p(N_2)$ if and only if there are

integers $a_i \equiv 1 \pmod{p}$ so that $a_1 + \cdots + a_k$ is even. We have assumed that p divides the number of edges of the graph, which is $k-1$. If $p = 2$, k is odd and there is no solution. If p is odd, we may take all $a_i = p + 1$.

For $G = K_1 \dot{\cup} K_{k-1}$, the rows of N_2 are all vectors of length k with $k-2$ 1's and two 0's. In this case, $\mathrm{row}_{\mathbb{Z}}(N_2)$ consists of all integer vectors $(a_1, \ldots, a_k)$ with $a_1 + \cdots + a_k \equiv 0 \pmod{k-2}$ and thus $\mathbb{1} \in \mathrm{row}_p(N_2)$ if and only if there are integers $a_i \equiv 1 \pmod{p}$ so that $a_1 + \cdots + a_k \equiv 0 \pmod{k-2}$. We have assumed that p divides the number of edges of the graph, which is $(k-1)(k-2)/2$. If p is an odd prime that divides $k-2$, then there is no solution $a_1, \ldots, a_k$ to the congruences. But otherwise, there do exist solutions (details omitted).

The remainder of the cases will use our results on fronts. First, we state a specialization of Lemma 2 for primes.

Lemma 26 *Let $EAF = D$ where E, F are unimodular and D integer diagonal with diagonal entries $d_1, \ldots, d_s$ (we understand $d_i = 0$ if $i > r$), and let p be a prime. Let $(c_1, \ldots, c_s) = \mathbb{1}F$. Then $\mathbb{1} \in \mathrm{row}_p(A)$ if and only if*

$$p \mid d_i \quad \textit{implies} \quad p \mid c_i.$$

Proof of Theorem 25 when G is primitive. We use the front E and diagonal form D given in Theorem 13. When both sides of $EN_2F = D$ are pre-multiplied by $(v, -\ell e/h, 0, \ldots, 0)$, we find

$$\mathbb{1}F = (vg/h, -\ell, 0, \ldots, 0).$$

The first two diagonal entries of D are eg/h and h. Note that if $p \nmid g$, then $p \nmid v$ since $p \mid e$ and $(a_1, g)/h \times v - \ell e/h \times u = 1$. Thus $p \nmid vg/h$ and $\mathbb{1} \notin \mathrm{row}_p(N_2(G))$. Note that vg/h and ℓ will not be 0 in $\mathbb{Z}_p$ together, otherwise we have $\mathbb{1} = \mathbf{0}$. Hence, $\mathbb{1} \in \mathrm{row}_p(N_2(G))$ if and only if $p \mid g$ and $p \nmid h$. □

Proof of Theorem 25 when $G = K_{r,k-r}$, $2 \le r \le k-2$. We use the front and diagonal factors given in Theorem 17. When both sides $EN_2F = D$ are pre-multiplied by $(1, -\ell e/h, 0, \ldots, 0)$, we find

$$\mathbb{1}F = (g/h, -\ell, 0, \ldots, 0).$$

The first two diagonal factors are eg/h and h. If $p \nmid g$, then $\mathbb{1} \notin \mathrm{row}_p(N_2(G))$. If $p \mid g = k-2r$, then together with $p \mid e = r(k-r)$, this implies $p \mid h = (r, k)$. However, g/h and ℓ will not both be 0 in $\mathbb{Z}_p$, otherwise we have $\mathbb{1} = \mathbf{0}$. Hence, $\mathbb{1} \notin \mathrm{row}_p(N_2(G))$. □

Proof of Theorem 25 when $G = K_r \dot\cup K_{k-r}$, $2 \le r \le k-2$. We use the fronts and diagonal factors given in Theorem 18.

First suppose that k is odd. When both sides of $EN_2F = D$ are pre-multiplied by $((1)^1, (-\ell e/h)^1, (0)^{\binom{k}{2}-5}, (-eg/h)^3)$, we find

$$\mathbb{1}F = ((2g/h)^1, (-\ell)^1, (0)^{\binom{k}{2}-5}, (-g/h)^3, 0, \ldots, 0).$$

Recall that the first two diagonal factors are $2eg/h$ and h, and the $(\binom{k}{2}-2)$-th through $\binom{k}{2}$-th diagonal factors are 1's. In this case, ℓ is even, so if $p = 2$, then $\mathbb{1} \in \mathrm{row}_p(N_2(G))$. If $p \mid g/h$, then $p \nmid \ell$ since $1 + \ell(r-1)/h \equiv 0 \pmod{g/h}$. Hence, $\mathbb{1} \in \mathrm{row}_p(N_2(G))$ if and only if $p \mid g$ and $p \nmid h$.

If k is even and $r - 1 \equiv h \pmod{2h}$, when both sides of $EN_2F = D$ are pre-multiplied by $((1)^1, (-\ell e/h)^1, (0)^{\binom{k}{2}-5}, (\ell e)^3)$, we find

$$\mathbb{1}F = ((g/h)^1, (-2\ell)^1, (0)^{\binom{k}{2}-5}, (\ell)^3, 0, \ldots, 0).$$

Recall that the first two diagonal factors are eg/h and $2h$, and the $(\binom{k}{2}-2)$-th through $\binom{k}{2}$-th diagonal factors are 1's. We claim that $k - r - 1 \equiv h \pmod{2h}$: if $r-1$ is odd, then $k-r-1$ is also odd; if $r-1$ is even, then $h \mid e = r(r-1)/2 + (k-r)(k-r-1)/2$ gives our result. Hence, $g = k - 2r \equiv 0 \pmod{2h}$, or g/h is even. If $p = 2$, $\mathbb{1} \in \mathrm{row}_p(N_2(G))$. If $p \mid g/h$, then $p \nmid \ell$ for the same reason as above, so $\mathbb{1} \in \mathrm{row}_p(N_2(G))$ if and only if $p \mid g$ and $p \nmid h$.

If k is even and $r - 1 \equiv 0 \pmod{2h}$, when $EN_2F = D$ is multiplied on both sides by $(1, -\ell e/h, 0, \ldots, 0)$, we find

$$\mathbb{1}F = (g/h, -2\ell, 0, \ldots, 0),$$

and the rest of the proof is the same as above. □

References

[1] N. Alon and Y. Caro, On three zero-sum Ramsey-type problems, *J. Graph Th.* **17** (1993), 177–192.

[2] A. E. Brouwer and C. A. van Eijl, On the p-rank of the adjacency matrices of strongly regular graphs, *J. Alg. Combinatorics* **1** (1992), 329–346.

[3] Y. Caro, A complete characterization of the zero-sum (mod 2) Ramsey Numbers, *J. Combinat. Thy. Ser. A* **68** (1994), 205–211.

[4] Y. Caro, Binomial coefficients and zero-sum Ramsey numbers, *J. Combinat. Thy. Ser. A* **80** (1997), 367–373.

[5] R. L. Graham, S.-Y. R. Li, and W.-C. W. Li, On the structure of t-designs, *SIAM J. Alg. Disc. Math.* **1** (1980), 8–14.

[6] J. E. Graver and W. B. Jurkat, The module structure of integral designs, *J. Combinat. Thy.* **15** (1973), 75–90.

[7] G. B. Khosrovshahi and Ch. Maysoori, On the bases for trades, *Linear Algebra and its Appl.* **226–228** (1995), 731–748.

[8] Morris Newman, The Smith normal form. Proceedings of the Fifth Conference of the International Linear Algebra Society (Atlanta, GA, 1995), *Linear Algebra and its Appl.* **254** (1997), 367–381.

[9] R. M. Wilson, A diagonal form for the incidence matrices of t-subsets vs. k-subsets, *Europ. J. Combinatorics* **11** (1990), 609–615.

[10] R. M. Wilson, On set systems with restricted intersections modulo p and p-ary t-designs. *Discrete Math.* **309** (2009), 606–612.

[11] R. M. Wilson, Signed hypergraph designs and diagonal forms for some incidence matrices. *Des. Codes Cryptogr.* **17** (1999) 289–297.

[12] R. M. Wilson, Some applications of incidence matrices of t-subsets and hypergraphs, Proceedings of the Third Shanghai Conference on Combinatorics, *Discrete Math.*, to appear.

[13] T. W. H. Wong, Ph.D. thesis, California Institute of Technology, to appear.